



Understanding the impacts of accurate Software Identification across the Software Lifecycle

Panel Discussion

Panelists

Steve Klos	TagVault.org	Executive Director
Roger Cummings	Symantec	Sr. Principal Software Engineer
Larry Wagoner	NSA	Technical Director, Supply Chain Risk Mgmt
Pat Cicala	Cicala & Associates	CEO & President
Richard Struse	DHS	Deputy Director for Software Assurance

Steve Klos - Background

- Executive director of TagVault.org
- Microsoft certified partner – SAM specialty
- Convener ISO/IEC 19770-2 development
- Member US TAG, WG-21 and SAM stds efforts
- Managing partner at Agnitio Advisors, Inc.

ISO/IEC 19770-2:2009

What does a SWID tag provide?

- Structured XML document
- Standardized software identification
- Supports suite/bundle identification
- Separate SW ID from entitlements
- Entitlement hints to SAM practitioners
- Move to automate compliance processes
- Supports software focused IT processes
- Supports various security requirements
- **Stop discovery through archeology**



TagVault.org

Actively Defining Requirements



IEEE-ISTO

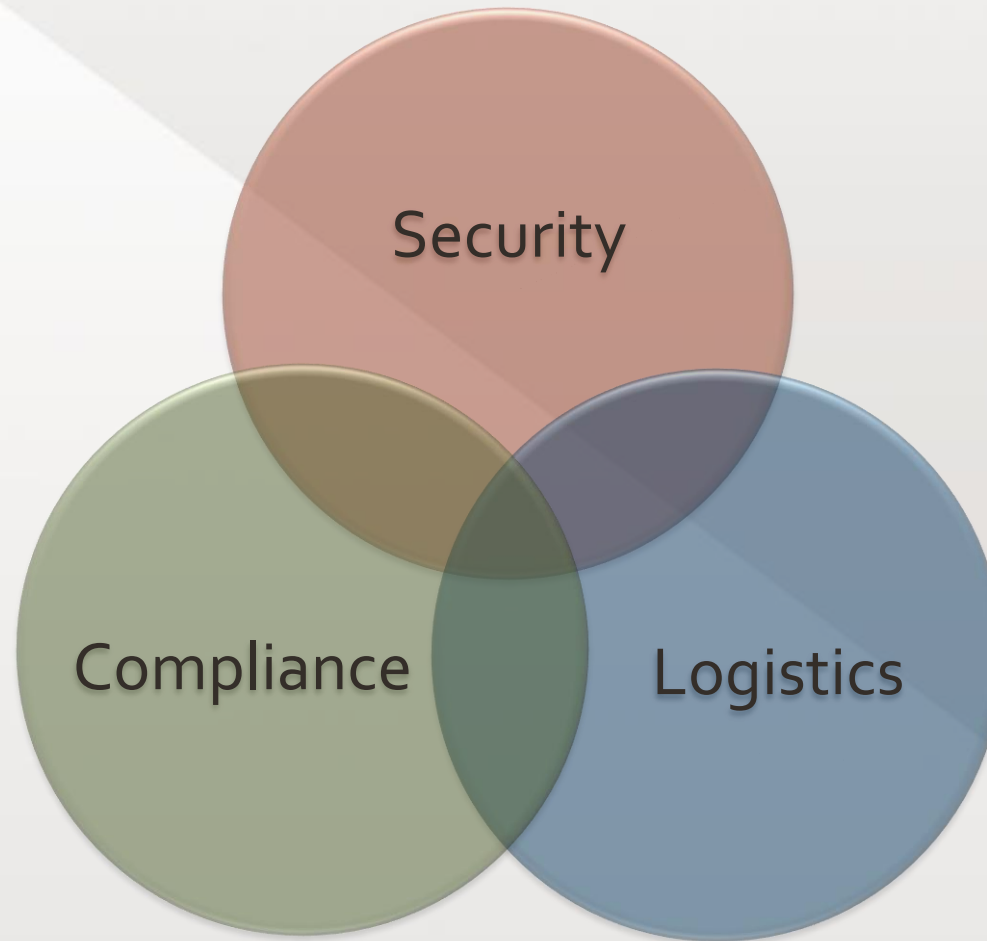
Industry Standards and Technology Organization
affiliated with the IEEE and the IEEE Standards Association

- Certification authority for software identification tags
- Non-profit
- Member driven
- Focus on market requirements (Authoritative and consistent)
- Supporting the SAM Eco-system
 - Certification process
 - Software tag repository
 - Software tools and services
 - Software ID tag best practices

TagVault.org is a 501(c) 6 program formed under IEEE-ISTO
(Industry Standards and Technology Organization)

Software Identification

Implications for the Software Lifecycle



Software Identification

Security Implications

- Supply Side Risk Management
 - Validation of installation media
 - Validate all files on installed media authoritatively match publishers specification
- Application/System Security
 - Rogue/changed/unauthorized files/applications
 - Validate that files associated with software application authoritatively match publisher specification
 - Ensuring fully patched systems
 - Patches are provided with details on which applications they apply to (no additional system scan required)
- Digital Signatures, timestamps
 - Provides authoritative data without necessarily requiring any external data source
 - Caveat – revocation of certs

Software Identification

Logistics Implications

- Software unique id (CPE) automation
 - Publisher creation of CPE names
 - Consistent and authoritative data provided
- Software identification for SCAP automation
 - No need to create archeological ID references in OVAL
- Additional and significant Meta data provided
 - Structural product relationships, abstract data, other materials
- Software purchasing
 - Single unique reference consistent for all purchasing, ordering, tracking & managing
- Software distribution and management
 - Explicit definition of software titles to distribute and ID
- Authoritative and consistent
 - Ensure reports, tools, systems, users are using the same data

Software Identification

Compliance Implications

- Consistency across agencies
 - Allows consolidation of data from various tools
- Software policy validation
 - Support for approved, unapproved and questionable software titles
- License Compliance/Optimization
 - Authoritative application ID – direct links to purchasing data
- Removing noise of application ID
 - Focus on titles that are licensed
 - Deal with underlying titles only if necessary
- Move to management by exception

Implementation Guide Development

US Based Technical Report

- US TAG approved development of national TR for SWID tag implementation guide
- TagVault.org will provide a significant amount of material to this effort
- Focused on industry/government/user requirements
- Will fast track to be ISO standard



Software Assurance Considerations for Certified ISO SWID Tags

Roger Cummings

Technical Director

Symantec Research Labs

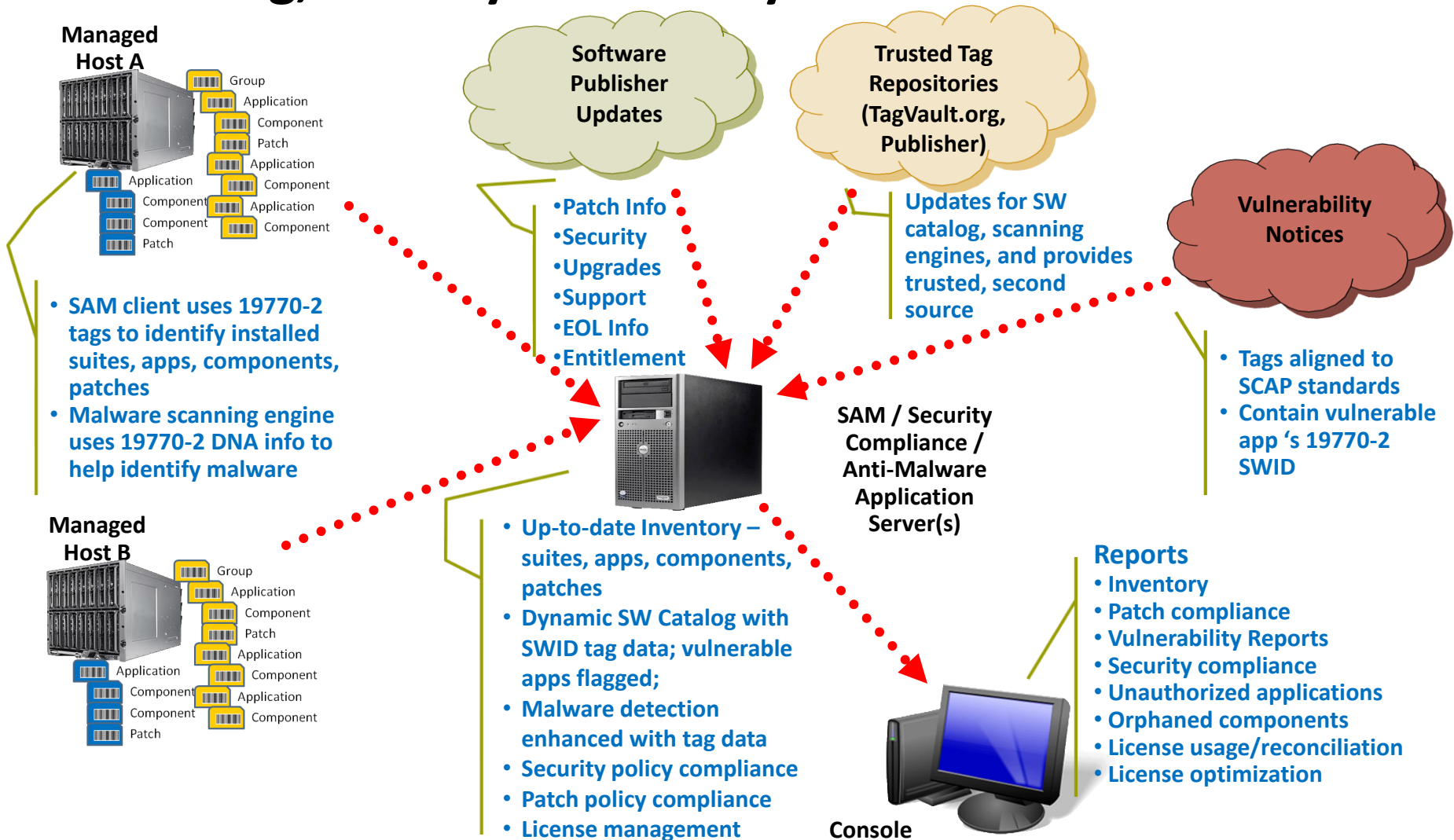
Software Assurance Forum – September 2011

Forward-looking Statements: *Any forward-looking indication of plans for products or programs is preliminary and all future release or delivery dates are tentative and are subject to change. Any future program plans, or release of a product or planned modifications to product capability, functionality, or feature are subject to ongoing evaluation by Symantec, and may or may not be implemented and should not be considered firm commitments by Symantec and should not be relied upon in making program participation or product purchasing decisions.*

Introduction

- Symantec has two different viewpoints on this work
 - Software Publisher
 - Tool Vendor
- I'm the lead for the US standards committee that tracks the ISO SC 7 WG21 Software Asset Management Group, plus:
 - US HoD to the ISO group
 - Secretary of the ISO group
 - Editor of 19770-5 Overview & Vocabulary standard

Certified tags provide the missing element for a self-sustaining, healthy SAM ecosystem ...



Manage more assets by exception, centrally ...

Host	Software Title	Version	Publisher	Security Alerts
Host-B	Storage Manager	2.0	StoreIT Corporation	Critical: Vulnerability CVE-2913-STIT-SM20 exists: Need patch iso-sid-patch-STIT-sm20-P1 to resolve.
Host-E	Personal ToolKit	6.0	LargeSoft	Critical: Installed application is missing one or more mandatory files
Host-G	MakeLotsOfDVDs	1.0	FreeToAll	Warning: Unauthorized application found
Host-J	Enterprise DB	9.0	Acme Corporation	Warning: System does not have required patch - iso-sid-app-acme-enterprise-db-v9-0-MP1
Host-J	Unknown	Unknown	Unknown	Critical: File scan detected executable files that do not match any ISO SW ID Tags
Host-P	Storage Manager	2.0	StoreIT Corporation	Critical: One or more executable files have been modified by a 3 rd party

Note: All products shown are fictional and are for example purposes only.

Difficult to secure/manage assets without up-to-date, consistent, normalized SW ID info from publishers ...

IT Requirements	Benefits of TagVault.org certified tags
Standard discovery	<ul style="list-style-type: none">• Standard XML files, in standard location• Same answer for all tools on all platforms
Single collection tool	<ul style="list-style-type: none">• Any and every tool collects the same information• Cross application, vendor, platform
Centralized reporting	<ul style="list-style-type: none">• Multiple tools fully supported, data consolidation• Data provided based on level of certification
Definitive and normalized data	<ul style="list-style-type: none">• Publisher provided data digitally signed• All common data values are normalized
Automation	<ul style="list-style-type: none">• Consistent and normalized data – easy automation• More software under management
Aligns with entitlement data	<ul style="list-style-type: none">• Minimized manual mapping of deployment data to entitlements• Designed to be “match-able” to future 19770-3 Entitlement tags
IT Process Integration	<ul style="list-style-type: none">• Definitive of apps, patches, etc., validation of install media integrity, DNA, ID of vulnerable apps pre/post install, etc. will greatly enhance config mgmt & security, budget, and help desk

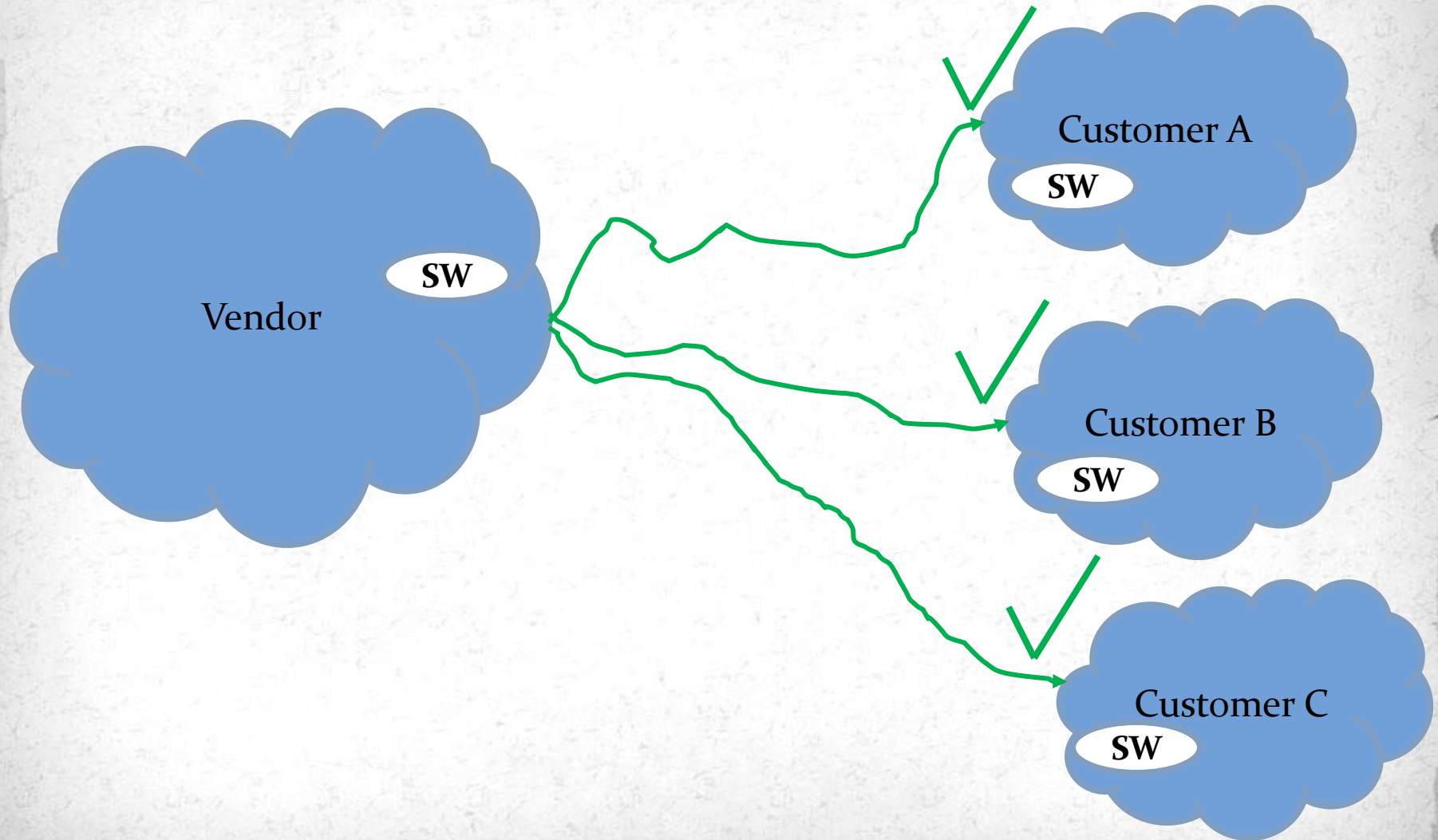
Software Tagging for Supply Chain Security

Larry Wagoner

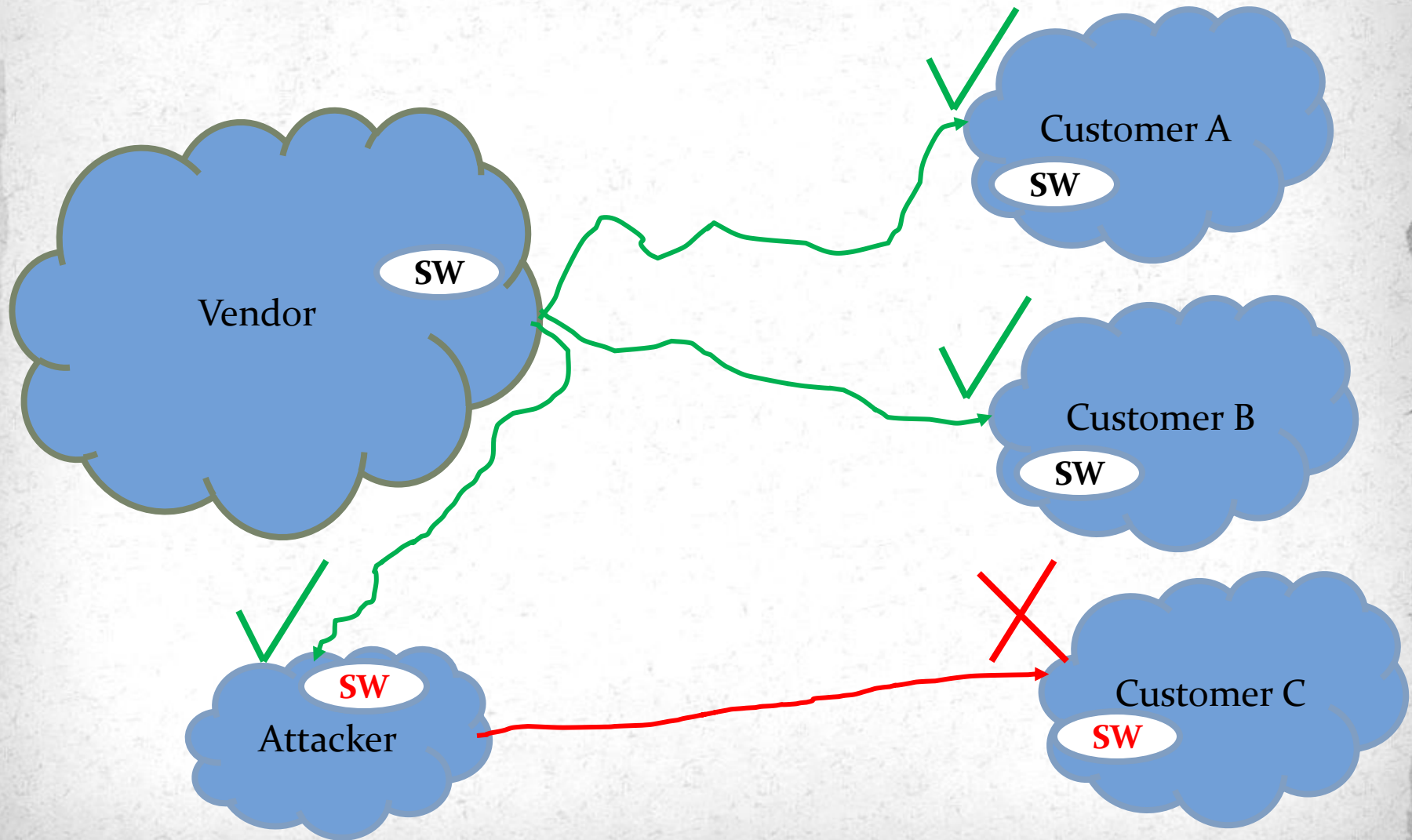
Good Software Assurance

- Necessary elements
 - Build it well
 - Ship it well
 - Use it well

Insecure Gap in Supply Chain



Insecure Gap in Supply Chain



Ship it well

- Challenge: How to Transport Software from the Vendor to the Customer Securely?
 - Shrink wrap it in plastic
 - Hmmm, won't work in Internet age
 - Look for solutions elsewhere
 - Abstract the problem
 - How to transport something of value from point A to point B?
 - Examine analogy
 - Use those lessons learned and transform back

Transporting Valuables



Supply Chain Situation



Wells Fargo Stagecoach Rules for Passenger Behavior

1. Abstinence from liquor is requested, but if you must drink share the bottle. To do otherwise makes you appear selfish and unneighborly.
2. If ladies are present, gentlemen are urged to forego smoking cigars and pipes as the odor of same is repugnant to the gentler sex. Chewing tobacco is permitted, but spit with the wind, not against it.
3. Buffalo robes are provided for your comfort in cold weather. Hogging robes will not be tolerated and the offender will be made to ride with the driver.
4. Don't snore loudly while sleeping or use your fellow passenger's shoulder for a pillow; he or she may not understand and friction may result.
5. Firearms may be kept on your person for use in emergencies. Do not fire them for pleasure or shoot at wild animals as the sound riles the horses.
6. In the event of runaway horses remain calm. Leaping from the coach in panic will leave you injured, at the mercy of the elements, hostile Indians and hungry coyotes.
7. Gents guilty of unchivalrous behavior toward lady passengers will be put off the stage. It's a long walk back. A word to the wise is sufficient.
8. Forbidden topics of conversation are: stagecoach robberies and Indian uprisings.

Ensuring the Supply Chain



Analogies

- Carrying valuables via (essentially) unprotected stagecoach
- Stagecoach robberies
- Armored Cars
- Shipping software unprotected over the Internet
- Malicious alteration of software in the supply chain
- Cryptographic protection of the software (digital code signing)

Digital Code Signing for Security

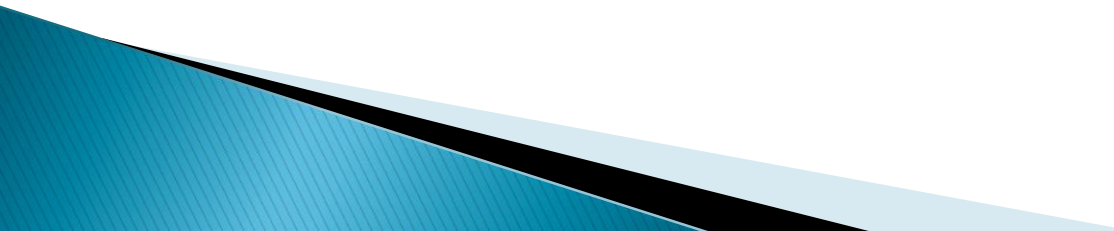
- Authenticate the source of the software
 - Need to identify the responsible party for the software
- No guarantee that the software is “good”
- No guarantee that the software will be used securely
- Only a guarantee that the software has not been altered since it left the vendor
 - But that fills a huge gap in security of the supply chain

Fundamental Building Block

- Multitude of uses once digital tagging is in place
- Secures not only initial software deliveries, but also patches and updates
- Can be used to periodically verify the integrity of a system
- Infrastructure to support digital code signing is useful for verifying cloud applications and even data

The end.

Panelist Data– Pat Cicala

- ▶ CEO & President Cicala & Associates
 - ▶ Have been in ITAM for 30 plus years
 - ▶ US Member of ISO
 - ▶ Working member of ISO WG21 and Convener of the 19770–7 Tag Management Technical Document Development Group
- 

Industry Drivers for Tagging

- ▶ There is no such thing as “Standard Data” in current software environments
- ▶ Translation of names, versions, license types platforms, etc. vary based on where the data originated and who is managing it
- ▶ There needs to be “True” authentication of data for many reasons

Industry Drivers For Tagging

- ▶ Facilitating more effective software life cycle management is no longer a “nice to have”
- ▶ The “buy/sell” relationships in software need to be improved and demystified
- ▶ Customers are becoming more sophisticated in their asset acquisition strategies and software assets have not kept pace

The entire software “Ecosystem” needs to get their act together!

An Industry View

The Future with Tagging

- ▶ Tagging will assist in all future SAM efforts for the publishers and customers that adopt tags
- ▶ Tags will “demystify” the software environment for all parties involved in the supply chain
- ▶ Ending the “mystery” behind software portfolios is a good not bad thing

An Industry View

The Future with Tagging

- ▶ Tagging will effect all aspects of the software lifecycle in a positive fashion
- ▶ Tagging may put a few “players” in the ecosystem out of business but this will ultimately enhance all spectrums of the “supply chain” increasing productivity, lowering costs and opening new market opportunities

Tagging if done and managed effectively will change the discipline of SAM and other IT processes for the foreseeable future!

Richard Struse

Deputy Director for Software Assurance

National Cyber Security Division
U.S. Department of Homeland Security

Richard.Struse@dhs.gov



Questions?



For further information contact:

Steve Klos
+1.732.562.6031

stevek@tagvault.org

www.tagvault.org

